DEPARTMENT PRIVACY AND SECURITY REQUIREMENTS

1. COMPLIANCE WITH STANDARDS AND DEPARTMENT REQUIEMENTS

1.1 The supplier is required to:

- Provide software that achieves a high level of security as measured against School requirements and relevant industry standards for security
- Internally implement and adhere to privacy and security principles in its operations and adheres to relevant industry standards for privacy and security

1.2 The Supplier acknowledges that its performance of Services under the Contract may involve access to confidential School information including, but not limited to, personally identifiable information, student education records, protected health information, or individual financial information (collectively, "Protected or Official Information as noted in the Department of Education's Information Classification Guidelines") that is subject to **Australian Privacy Law** restricting the use and disclosure of such information.

1.3 The Supplier is expected to comply with the Victorian Protective Data Security Framework (VPDSF) and meet the standards below:

- Payment Card Industry Data Security Standard (PCI DSS) (where applicable)
- National Institute of Standards and Technology (NIST)
- Australian Signals Directorate Information Security Manual(ASD ISM)

1.4 The supplier and its solutions will be subject to and must comply with a School security assessment which is based on the Victorian Protective Security Standards as documented in the School security assessment tool involving privacy and security questions and evidence as required.

1.5 The supplier's internal operations and its solutions must comply with the Information Privacy Principles set out under the *Privacy and Data Protection Act 2014* (Vic) available at the following webpage: https://www.cpdp.vic.gov.au/menu-law-enforcement/law-enforcement-standards.

2. PRIVACY/SECURITY INCIDENTS

2.1 The Service Provider must immediately notify the School in writing (and include all known details) of a Privacy Incident.

2.2 The School may request the Service Provider to provide further details in relation to the Privacy Incident.

2.3 The Service Provider must, as soon as reasonably possible (and, in any event, within five (5) Business Days) of receiving a request from the School, provide all of the details requested by the School.

2.4 The School will then notify the Service Provider, in writing of the action the Service Provider must take in relation to the Privacy Incident and upon receiving such notice, the Service Provider must undertake all the actions required in the notice.

2.5 The Service Provider agrees that it shall not inform any third party of any Security Breach without first obtaining the School's prior written consent, other than to inform a complainant that the matter has been forwarded to Customer's legal counsel.

3. CO-ORDINATION OF BREACH RESPONSE ACTIVITIES

In the event of a Breach, The Supplier will:

3.1 Immediately preserve any potential forensic evidence relating to the breach.

3.2 Promptly designate a contact person to whom the School will direct inquiries, and who will communicate Contractor responses to the School inquiries.

3.3 As rapidly as circumstances permit, apply appropriate resources to remedy the breach condition, investigate, document, restore the School service(s) as directed by the School, and undertake appropriate response activities.

3.4 Provide status reports to the School on Breach response activities, either on a daily basis or a frequency approved by the School.

3.5 Coordinate all media, law enforcement, or other Breach notifications with the School in advance of such notification(s), unless expressly prohibited by law.

3.6 Make all reasonable efforts to assist and cooperate with the School in its Breach response efforts.

3.7 Ensure that knowledgeable staff are available on short notice, if needed, to participate in the School initiated meetings and/or conference calls regarding the Breach.